

The Geometry of Homogeneous Two-Weight Codes

Thomas Honold

ABSTRACT. The results of [1, 2] on linear homogeneous two-weight codes over finite Frobenius rings are extended in two ways: It is shown that certain non-projective two-weight codes give rise to strongly regular graphs in the way described in [1, 2]. Secondly, these codes are used to define a dual two-weight code and strongly regular graph similar to the classical case of projective linear two-weight codes over finite fields [3].

1. Introduction

A finite ring R is said to be a Frobenius ring if there exists a character $\chi \in \widehat{R} = \text{Hom}_{\mathbb{Z}}(R, \mathbb{C}^\times)$ whose kernel contains no nonzero left (or right) ideal of R . The (normalized) homogeneous weight $w_{\text{hom}}: R \rightarrow \mathbb{C}$ on a finite Frobenius ring R is defined by

$$w_{\text{hom}}(x) = 1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(ux). \quad (1)$$

(This does not depend on the choice of χ .) The function w_{hom} is the unique complex-valued function on R satisfying $w_{\text{hom}}(0) = 0$, $w_{\text{hom}}(ux) = w_{\text{hom}}(x)$ for $x \in R$, $u \in R^\times$ and $\sum_{x \in I} w_{\text{hom}}(x) = |I|$ for all nonzero left ideals $I \leq_R R$ (and their right counterparts).

The homogeneous weight on a finite Frobenius ring is a generalization of both the Hamming weight on \mathbb{F}_q ($w_{\text{hom}}(x) = \frac{q}{q-1} w_{\text{Ham}}(x)$ for $x \in \mathbb{F}_q$) and the Lee weight on \mathbb{Z}_4 ($w_{\text{hom}}(x) = w_{\text{Lee}}(x)$ for $x \in \mathbb{Z}_4$). It was introduced in [4] for the case $R = \mathbb{Z}_m$ and generalized to Frobenius rings in [6, 9].

In [1, 2] it was shown that a linear code C over a finite Frobenius ring with exactly two nonzero homogeneous weights and satisfying certain nondegeneracy conditions gives rise to a strongly regular graph with C as its set of vertices. In the classical case $R = \mathbb{F}_q$ this result has been known for a long time and forms part of the more general correspondence between projective linear $[n, k]$ two-weight codes and $\{\lambda_1, \lambda_2\}$ difference sets over \mathbb{F}_q and their (appropriately defined) duals (cf. [3, 5]).

In this paper we generalize the results of [1, 2] to a larger class of homogeneous two-weight codes (so-called modular two-weight codes) and establish for these codes the classical correspondence (Theorems 3.2 and 5.7 of [3]) in full generality.

2. A few properties of Frobenius rings and their homogeneous weights

For a subset S of a ring R let ${}^\perp S = \{x \in R; xS = 0\}$, $S^\perp = \{x \in R; Sx = 0\}$. Similarly, for $S \subseteq R^n$ let ${}^\perp S = \{\mathbf{x} \in R^n; \mathbf{x} \cdot S = 0\}$ and $S^\perp = \{\mathbf{x} \in R^n; S \cdot \mathbf{x} = 0\}$, where $\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$.

2000 *Mathematics Subject Classification.* Primary 94B05; Secondary 05E30, 05B10.

Key words and phrases. Codes over Frobenius rings, homogeneous weight, two-weight code, modular code, strongly regular graph, partial difference set.

Expanded version with proofs of *Further Results on Homogeneous Two-Weight Codes*, which appeared in the OC2007 conference proceedings.

PROPOSITION 1. A finite ring R is a Frobenius ring iff for every matrix $\mathbf{A} \in R^{m \times n}$ the left row space $C = \{\mathbf{x}\mathbf{A}; \mathbf{x} \in R^m\}$ and the right column space $D = \{\mathbf{A}\mathbf{y}; \mathbf{y} \in R^n\}$ have the same cardinality.

PROOF. Suppose first that R is Frobenius. The map $R^n \rightarrow R^m$, $\mathbf{y} \mapsto \mathbf{A}\mathbf{y}$ has kernel C^\perp and image D . By the homomorphism theorem, $|C^\perp||D| = |R^n|$. Thus $|C| = |D|$ iff $|C||C^\perp| = |R^n|$. Since finite Frobenius rings are characterized by the property that $|C||C^\perp| = |R^n|$ for every n and every submodule $|C| \leq_R R^n$ (cf. for example [8]), the result follows. \square

From now on we suppose that R is a finite Frobenius ring with homogeneous weight w_{hom} . First we recall an alternative expression for $w_{\text{hom}}(x)$ derived in [9]. Suppose $R/\text{rad } R = \prod_{i=1}^t R_i$ where $R_i \cong M(m_i, \mathbb{F}_{q_i})$ is a simple ring and $|R_1| \leq |R_2| \leq \dots \leq |R_t|$. Then $\text{soc}(R) = \bigoplus_{i=1}^t S_i$ where $S_i \cong R_i$ (as an R_i - R_i -bimodule) is the two-sided ideal of R defined by $R_i S_i = S_i R_i = S_i$ and $R_i S_j = S_j R_i = \{0\}$ for $1 \leq i, j \leq t$.

From [9] we have the following: If $x \notin \text{soc}(R)$ then $w_{\text{hom}}(x) = 1$. If $x \in \text{soc}(R)$, $x = \sum_{i=1}^t x_i$ with $x_i \in S_i$, then

$$w_{\text{hom}}(x) = 1 - \prod_{i=1}^t \frac{(-1)^{\text{rk } x_i}}{(q_i^{m_i} - 1)(q_i^{m_i-1} - 1) \dots (q_i^{m_i - \text{rk } x_i + 1} - 1)}, \quad (2)$$

where $\text{rk}: S_i \rightarrow \mathbb{N}_0$ denotes the “matrix rank” induced by the isomorphism $S_i \cong M(m_i, \mathbb{F}_{q_i})$.

Next we determine the set of all $x \in R$ satisfying $w_{\text{hom}}(x) = 0$. Let $S_i = R s_i$, $1 \leq i \leq \tau$, be the different left ideals of R of order 2 and $S = S_1 + \dots + S_\tau$. The set S is a two-sided ideal of R of order 2^τ , whose elements are the subset sums of $\{s_1, \dots, s_\tau\}$. Define $S_0 \subseteq S$ as the set of all sums of an even number of elements from $\{s_1, \dots, s_\tau\}$ (“even-weight subcode of S ”). Note that S_0 is a subgroup of $(R, +)$, trivial for $\tau \leq 1$ and nontrivial (of order $2^{\tau-1}$) for $\tau \geq 2$.

PROPOSITION 2. We have $w_{\text{hom}}(x) \geq 0$ for all $x \in R$ and $S_0 = \{x \in R; w_{\text{hom}}(x) = 0\}$. Moreover, $w_{\text{hom}}(x + y) = w_{\text{hom}}(x)$ for all $x \in R$ and $y \in S_0$.

PROOF. This follows from a close inspection of the formula (2). \square

FACT 3 (cf. [7]).

$$\sum_{x \in I} w_{\text{hom}}(x + c) = |I| \quad (3)$$

for all nonzero left (or right) ideals I of R and all $c \in R$.

The following correlation property of w_{hom} turns out to be crucial.

PROPOSITION 4. For a nonzero left ideal I of R and $r, s \in R$ we have

$$\sum_{x \in I} w_{\text{hom}}(x) w_{\text{hom}}(xr + s) = \begin{cases} |I| + |I| \cdot \frac{|R^\times \cap (1+I^\perp)|}{|R^\times|} \cdot (1 - w_{\text{hom}}(s)) & \text{if } |Ir| = |I|, \\ |I| & \text{if } |Ir| < |I|. \end{cases} \quad (4)$$

In particular $\sum_{x \in R} w_{\text{hom}}(x)^2 = |R| \cdot \left(1 + \frac{1}{|R^\times|}\right)$.

PROOF. Denote the left-hand side of (4) by $\rho(s)$. Using (3) it is easily verified that $\rho(us) = \rho(s)$ for $s \in R$, $u \in R^\times$ and $\sum_{s \in J} \rho(s) = |I||J|$ for all nonzero left ideals $J \leq_R R$. Hence $\rho(s) = \rho(0) + (|I| - \rho(0)) w_{\text{hom}}(s)$ for $s \in R$.

If $|Ir| < |I|$ then $K := I \cap {}^\perp r \neq 0$. Hence choosing $x_a \in I$ with $x_a r = a$ (for $a \in Ir$) we get

$$\begin{aligned} \rho(0) &= \sum_{x \in I} w_{\text{hom}}(x) w_{\text{hom}}(xr) = \sum_{a \in Ir} \left(\sum_{x \in K + x_a} w_{\text{hom}}(x) \right) w_{\text{hom}}(a) \\ &= |K| \sum_{a \in Ir} w_{\text{hom}}(a) = |K||Ir| = |I|. \end{aligned}$$

If $|Ir| = |I|$, i. e. $I \rightarrow Ir$, $x \mapsto xr$ is an isomorphism of left R -modules, then $w_{\text{hom}}(xr) = w_{\text{hom}}(x)$ and hence

$$\begin{aligned}
\rho(0) &= \sum_{x \in I} w_{\text{hom}}(x)^2 = \sum_{x \in I} \left(1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(xu) \right)^2 \\
&= |I| + \frac{1}{|R^\times|^2} \cdot \sum_{u, v \in R^\times} \sum_{x \in I} \chi(x(u+v)) \\
&= |I| + \frac{|I|}{|R^\times|^2} \cdot |\{(u, v) \in R^\times \times R^\times; I(u+v) = 0\}| \\
&= |I| + \frac{|I|}{|R^\times|} \cdot |\{u \in R^\times; I(u-1) = 0\}| \\
&= |I| + \frac{|I|}{|R^\times|} \cdot |R^\times \cap (1 + I^\perp)|.
\end{aligned}$$

□

For vectors $\mathbf{x}, \mathbf{y} \in R^k$ we write $\mathbf{x} \sim \mathbf{y}$ if $\mathbf{x}R^\times = \mathbf{y}R^\times$. By [11, Prop. 5.1] this is equivalent to $\mathbf{x}R = \mathbf{y}R$.

PROPOSITION 5. For nonzero words $\mathbf{g}, \mathbf{h} \in R^k$ and $s \in R$ we have

$$\sum_{\mathbf{x} \in R^k} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}) w_{\text{hom}}(\mathbf{x} \cdot \mathbf{h} + s) = \begin{cases} |R|^k + \frac{|R|^k}{|\mathbf{g}R^\times|} \cdot (1 - w_{\text{hom}}(s)) & \text{if } \mathbf{g} \sim \mathbf{h}, \\ |R|^k & \text{if } \mathbf{g} \not\sim \mathbf{h}. \end{cases} \quad (5)$$

PROOF. Reasoning as in the proof of Prop. 4 the left-hand side $\rho(s)$ of (5) satisfies $\rho(s) = \rho(0) + (|R|^k - \rho(0))w_{\text{hom}}(s)$ for $s \in R$.

For $\mathbf{g} \in R^k$, $a \in R$ the equation $\mathbf{x} \cdot \mathbf{g} = x_1g_1 + \dots + x_kg_k = a$ is solvable if and only if $a \in Rg_1 + \dots + Rg_k$. If this is true and \mathbf{x}_a denotes a particular solution, the set of all solutions is the coset $\mathbf{x}_a + {}^\perp\mathbf{g}$. Hence

$$\rho(0) = \sum_{\mathbf{x} \in R^k} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}) w_{\text{hom}}(\mathbf{x} \cdot \mathbf{h}) = \sum_{a \in Rg_1 + \dots + Rg_k} w_{\text{hom}}(a) \sum_{\mathbf{y} \in {}^\perp\mathbf{g}} w_{\text{hom}}((\mathbf{x}_a + \mathbf{y}) \cdot \mathbf{h}). \quad (6)$$

There are now two cases to consider.

Case (i): $\mathbf{h} \in \mathbf{g}R = ({}^\perp\mathbf{g})^\perp$. Letting $\mathbf{h} = \mathbf{g}r$ we have $(\mathbf{x}_a + \mathbf{y}) \cdot \mathbf{h} = (\mathbf{x}_a \cdot \mathbf{g})r + (\mathbf{y} \cdot \mathbf{g})r = ar$ for all $\mathbf{y} \in {}^\perp\mathbf{g}$ and hence

$$\rho(0) = |{}^\perp\mathbf{g}| \cdot \sum_{a \in Rg_1 + \dots + Rg_k} w_{\text{hom}}(a) w_{\text{hom}}(ar).$$

If $\mathbf{h}R = \mathbf{g}R$, we may assume $r \in R^\times$. Applying Proposition 4 to $I = Rg_1 + \dots + Rg_k$ and using $|{}^\perp\mathbf{g}||I| = |{}^\perp\mathbf{g}||Rg_1 + \dots + Rg_k| = |R|^k$, $I^\perp = \{r \in R; g_1r = \dots = g_kr = 0\} = \{r \in R; \mathbf{g}r = \mathbf{0}\}$, $R^\times \cap (1 + I^\perp) = R^\times \cap (1 + \mathbf{g}^\perp) = \{u \in R^\times; \mathbf{g}u = \mathbf{g}\}$ gives

$$\begin{aligned}
\rho(0) &= |{}^\perp\mathbf{g}| \cdot \sum_{a \in I} w_{\text{hom}}(a)^2 = |R|^k + |R|^k \cdot \frac{|\{u \in R^\times; \mathbf{g}u = \mathbf{g}\}|}{|R^\times|} \\
&= |R|^k + \frac{|R|^k}{|\mathbf{g}R^\times|}
\end{aligned}$$

as desired. Otherwise $\mathbf{h}R = \mathbf{g}rR \subsetneq \mathbf{g}R$, ${}^\perp\mathbf{g} \subsetneq {}^\perp(\mathbf{g}r)$ and hence there exists $\mathbf{x} \in R^k$ such that $a := x_1g_1 + \dots + x_kg_k \neq 0$, $ar = x_1g_1r + \dots + x_kg_kr = 0$. Thus $|Ir| < |I|$, and Proposition 4 then implies

$$\rho(0) = |{}^\perp\mathbf{g}| \cdot |I| = |R|^k.$$

Case (ii): $\mathbf{h} \notin \mathbf{g}R$. Here $\mathbf{x}_a \cdot \mathbf{h} + {}^\perp \mathbf{g} \cdot \mathbf{h}$ is a coset of a nonzero left ideal of R and hence

$$\rho(0) = |{}^\perp \mathbf{g}| \cdot \sum_{a \in Rg_1 + \dots + Rg_k} w_{\text{hom}}(a) = |{}^\perp \mathbf{g}| \cdot |Rg_1 + \dots + Rg_k| = |R^k|, \quad (7)$$

completing the proof of Prop. 5. \square

3. Modular Two-Weight Codes, Partial Difference Sets and Strongly Regular Graphs

Given a positive integer k , the set of nonzero cyclic submodules of the free right module R_R^k is denoted by \mathcal{P} . The elements of \mathcal{P} are referred to as *points* of the projective geometry $\text{PG}(R_R^k)$, and a multiset $\alpha: \mathcal{P} \rightarrow \mathbb{N}_0$ is referred to as a *multiset in* $\text{PG}(R_R^k)$.

With a left linear code $C \leq {}_R R^n$ generated by k (or fewer) codewords and having no all-zero coordinate we associate a multiset α_C in $\text{PG}(R_R^k)$ of cardinality n in the following way: If $C = \{\mathbf{x}\mathbf{G}; \mathbf{x} \in R^k\}$ with $\mathbf{G} = (\mathbf{g}_1 | \mathbf{g}_2 | \dots | \mathbf{g}_n) \in R^{k \times n}$, define $\alpha_C: \mathcal{P} \rightarrow \mathbb{N}_0$ by $\alpha_C(\mathbf{g}R) = |\{j; \mathbf{g}_j R = \mathbf{g}R\}|$. The relation $C \leftrightarrow \alpha_C$ defines a bijection between classes of monomially isomorphic left linear codes over R generated by k codewords and orbits of the group $\text{GL}(k, R)$ on multisets in $\text{PG}(R_R^k)$.

DEFINITION 6. A code $C \leq {}_R R^n$ is said to be *modular* if there exists $r \in \mathbb{Q}$ such that for all points $\mathbf{g}R$ of $\text{PG}(R_R^k)$ either $\alpha_C(\mathbf{g}R) = 0$ or $\alpha_C(\mathbf{g}R) = r|\mathbf{g}R^\times|$. The number r is called the *index* of C .

The property of C described in Def. 6 does not depend on the choice of α_C (not even on the dimension k). Hence modularity of a linear code is a well-defined concept.

If $A \subseteq R^k \setminus \{\mathbf{0}\}$ satisfies $AR^\times = A$, the matrix \mathbf{G} with the vectors of A as columns generates a modular (left) linear code of length $|A|$ and index 1.

Note that projective codes over \mathbb{F}_q are modular of index $\frac{1}{q-1}$ and regular projective codes over R as defined in [1, 2] are modular of index $\frac{1}{|R^\times|}$.

FACT 7 ([12, Th. 5.4]). A linear code $C \leq {}_R R^n$ is a one-weight code (i. e. equidistant w. r. t. w_{hom}) iff C is modular and $\{\mathbf{g} \in R^k \setminus \{\mathbf{0}\}; \alpha_C(\mathbf{g}R) > 0\}$ is the set of nonzero vectors of a submodule of R_R^k .

The main purpose of this paper is a combinatorial characterization of (linear) homogeneous two-weight codes over R , i. e. codes over R having exactly two nonzero homogeneous weights $w_1 < w_2$. Assuming that C is such a code, we set $w_0 = 0$, $C_i = \{\mathbf{c} \in C; w_{\text{hom}}(\mathbf{c}) = w_i\}$ and $b_i = |C_i|$ for $i = 0, 1, 2$.

By Prop. 2 we have $w_{\text{hom}}(\mathbf{c}) = 0$ iff $w_{\text{hom}}(c_j) = 0$ for $1 \leq j \leq n$, the set C_0 is a subgroup of $(C, +)$ and C_1, C_2 are unions of cosets of C_0 . If the weights w_1, w_2 and $b_0 = |C_0|$ are known, the frequencies b_1, b_2 can be computed from the equations $b_1 + b_2 = |C| - |C_0|$, $b_1 w_1 + b_2 w_2 = \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) = n|C|$ (assuming that C has no all-zero coordinate) and are given by

$$b_1 = \frac{(w_2 - n)|C| - w_2|C_0|}{w_2 - w_1}, \quad b_2 = \frac{(n - w_1)|C| + w_1|C_0|}{w_2 - w_1}. \quad (8)$$

LEMMA 8. For a modular code $C \leq {}_R R^n$ of index r and $\mathbf{d} \in R^n$ we have

$$\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(\mathbf{c} + \mathbf{d}) = |C| \cdot (n^2 + rn - r \cdot w_{\text{hom}}(\mathbf{d})).$$

PROOF. Suppose that C is generated by $\mathbf{G} = (\mathbf{g}_1 | \dots | \mathbf{g}_n) \in R^{k \times n}$. By assumption, the multiset α in $\text{PG}(R_R^k)$ obtained from \mathbf{G} satisfies $\alpha(\mathbf{g}_j R) = r|\mathbf{g}_j R^\times|$ for $1 \leq j \leq n$. We obtain

$$\begin{aligned}
\frac{1}{|C|} \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(\mathbf{c} + \mathbf{d}) &= \frac{1}{|R|^k} \sum_{\mathbf{x} \in R^k} w_{\text{hom}}(\mathbf{xG}) w_{\text{hom}}(\mathbf{xG} + \mathbf{d}) \\
&= \frac{1}{|R|^k} \sum_{i,j=1}^n \sum_{\mathbf{x} \in R^k} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}_i) w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}_j + d_j) \\
&= n^2 + \sum_{j=1}^n \frac{1 - w_{\text{hom}}(d_j)}{|\mathbf{g}_j R^\times|} \times \#\{i; \mathbf{g}_i \sim \mathbf{g}_j\} \quad (\text{by Prop. 5}) \\
&= n^2 + \sum_{j=1}^n \frac{1 - w_{\text{hom}}(d_j)}{|\mathbf{g}_j R^\times|} \times \alpha(\mathbf{g}_j R) \\
&= n^2 + rn - r \cdot w_{\text{hom}}(\mathbf{d})
\end{aligned}$$

as asserted. \square

In the special case $\mathbf{d} = \mathbf{0}$ Lemma 8 reduces to $\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c})^2 = (n^2 + rn)|C|$.

LEMMA 9. *The nonzero weights w_1, w_2 of a modular two-weight code $C \leq_R R^n$ of index r satisfy the relation*

$$(w_1 + w_2)n|C| = (n^2 + rn)|C| + w_1 w_2(|C| - |C_0|).$$

PROOF. We have the system

$$\begin{aligned}
b_1 + b_2 &= |C| - |C_0|, \\
b_1 w_1 + b_2 w_2 &= n|C|, \\
b_1 w_1^2 + b_2 w_2^2 &= (n^2 + rn)|C|,
\end{aligned}$$

from which we obtain the asserted formula using

$$(w_1 + w_2)(b_1 w_1 + b_2 w_2) = (b_1 w_1^2 + b_2 w_2^2) + w_1 w_2(b_1 + b_2).$$

\square

LEMMA 10. *For a modular two-weight code $C \leq_R R^n$ of index r and $\mathbf{d} \in R^n$ we have*

$$\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) = b_1 w_1 + \left(b_1 - \frac{b_1 w_1}{n}\right) w_{\text{hom}}(\mathbf{d}) \quad (9)$$

PROOF. Using Lemma 8 we can setup the following system of equations for the unknowns $\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(\mathbf{c} + \mathbf{d})$ and $\sum_{\mathbf{c} \in C_2} w_{\text{hom}}(\mathbf{c} + \mathbf{d})$:

$$\begin{aligned}
\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) + \sum_{\mathbf{c} \in C_2} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) &= \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) - \sum_{\mathbf{c} \in C_0} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) \\
&= n|C| - |C_0| w_{\text{hom}}(\mathbf{d}), \\
w_1 \sum_{\mathbf{c} \in C_1} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) + w_2 \sum_{\mathbf{c} \in C_2} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) &= \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(\mathbf{c} + \mathbf{d}) \\
&= |C| \cdot (n^2 + rn - r \cdot w_{\text{hom}}(\mathbf{d}))
\end{aligned}$$

Solving this system yields

$$\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(\mathbf{c} + \mathbf{d}) = \frac{(w_2 n - n^2 - rn)|C|}{w_2 - w_1} + \frac{r|C| - w_2|C_0|}{w_2 - w_1} \cdot w_{\text{hom}}(\mathbf{d}) \quad (10)$$

for any $\mathbf{d} \in R^n$. The first summand in (10) is equal to $b_1 w_1$, as follows by inserting $\mathbf{d} = \mathbf{0}$. This in turn gives

$$b_1 - \frac{b_1 w_1}{n} = \frac{(w_2 - n)|C| - w_2|C_0|}{w_2 - w_1} - \frac{(w_2 - n - r)|C|}{w_2 - w_1} = \frac{r|C| - w_2|C_0|}{w_2 - w_1},$$

transforming (10) into (9). □

REMARK 11. Lemmas 8 and 10 can be generalized to

$$\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(c_j + d_j) = |C| \cdot (n + r - r \cdot w_{\text{hom}}(d_j)) \quad \text{and}$$

$$\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(c_j + d_j) = \frac{b_1 w_1}{n} + \left(b_1 - \frac{b_1 w_1}{n} \right) w_{\text{hom}}(d_j)$$

respectively, where j is any coordinate of R^n and $d_j \in R$. In particular $\sum_{\mathbf{c} \in C_1} w_{\text{hom}}(c_j) = \frac{b_1 w_1}{n}$ is independent of j .

Recall that a (simple) graph Γ is *strongly regular with parameters* (N, K, λ, μ) if Γ has N vertices, is regular of degree K and any two adjacent (resp. nonadjacent) vertices have λ (resp. μ) common neighbours. The graph Γ is called *trivial* if Γ or its complement is a disjoint unions of cliques of the same size. This is equivalent to $\mu = 0$ resp. $\mu = K$.

A subset $D \subset G$ of an (additively written) abelian group G is said to be a *regular* (N, K, λ, μ) *partial difference set in* G if $N = |G|$, $K = |D|$, $0 \notin D$, $-D = D$, and the multiset $D - D$ represents each element of D exactly λ times and each element of $G \setminus (D \cup \{0\})$ exactly μ times; cf. [10].

If D is a regular (N, K, λ, μ) partial difference set in G , then the graph $\Gamma(G, D)$ with vertex set G and edge set $\{\{x, x + d\}; x \in G, d \in D\}$ (the *Cayley graph* of G w. r. t. D) is strongly regular with parameters (N, K, λ, μ) .

We are now ready to generalize the main result of [2, 1] to modular two-weight codes. For a two-weight code C we denote the Cayley graph $\Gamma(C/C_0, C_1/C_0)$ by $\Gamma(C)$. Thus the vertices of $\Gamma(C)$ are the cosets of C_0 in C , and two cosets $\mathbf{c} + C_0, \mathbf{d} + C_0$ are adjacent iff $w_{\text{hom}}(\mathbf{c} - \mathbf{d}) = w_1$. As we have already mentioned, Prop. 2 ensures that $\Gamma(C)$ is well-defined.

THEOREM 12. *The graph $\Gamma(C)$ associated with a modular two-weight code over a finite Frobenius ring R is strongly regular with parameters*

$$N = \frac{|C|}{|C_0|}, \quad K = \frac{(w_2 - n)N - w_2}{w_2 - w_1},$$

$$\lambda = \frac{K \left(\frac{w_1^2}{n} - 2w_1 \right) + w_2(K - 1)}{w_2 - w_1}, \quad \mu = \frac{K \left(\frac{w_1 w_2}{n} - w_1 - w_2 \right) + w_2 K}{w_2 - w_1}.$$

The graph $\Gamma(C)$ is trivial iff $w_1 = n$.

PROOF. The numbers $b_i = |C_i|$ satisfy the system of equations

$$\begin{aligned} b_1 + b_2 &= |C| - |C_0|, \\ w_1 b_1 + w_2 b_2 &= \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) = n|C|, \end{aligned}$$

giving

$$\begin{pmatrix} b_1 \\ b_2 \end{pmatrix} = \frac{1}{w_2 - w_1} \begin{pmatrix} (w_2 - n)|C| - w_2|C_0| \\ (n - w_1)|C| + w_1|C_0| \end{pmatrix} \quad \text{and} \quad K = b_1/b_0 = \frac{(w_2 - n)N - w_2}{w_2 - w_1}.$$

Let now $b_{ij}(\mathbf{d}) = |C_i \cap (C_j + \mathbf{d})| = |\{\mathbf{c} \in C_i; w_{\text{hom}}(\mathbf{c} - \mathbf{d}) = w_j\}|$ for $\mathbf{d} \in C$ and $0 \leq i, j \leq 2$. Our task is to show that $b_{11}(\mathbf{d})$ depends only on the class C_i containing \mathbf{d} . The cases $i = 0$, $j = 0$ and $\mathbf{d} \in C_0$ are trivial. The numbers $b_{11}(\mathbf{d})$, $b_{12}(\mathbf{d})$ are the solutions of the system of equations

$$b_{11}(\mathbf{d}) + b_{12}(\mathbf{d}) = |C_1| - |C_1 \cap (C_0 + \mathbf{d})| = \begin{cases} |C_1| - |C_0| & \text{if } \mathbf{d} \in C_1, \\ |C_1| & \text{if } \mathbf{d} \in C_2, \end{cases}$$

$$w_1 \cdot b_{11}(\mathbf{d}) + w_2 \cdot b_{12}(\mathbf{d}) = \sum_{\mathbf{c} \in C_1} w_{\text{hom}}(\mathbf{c} - \mathbf{d}),$$

whose coefficient matrix depends only on $w_{\text{hom}}(\mathbf{d})$; cf. Lemma 10. This proves already that $\Gamma(C)$ is strongly regular with parameters $\lambda = b_{11}(\mathbf{d})/|C_0|$ and $\mu = b_{11}(\mathbf{d}')/|C_0|$, where $\mathbf{d} \in C_1$, $\mathbf{d}' \in C_2$. Using Lemma 10 we find

$$\begin{aligned}\lambda &= \frac{w_2(b_1 - b_0) - b_1 w_1 - \left(b_1 - \frac{b_1 w_1}{n}\right) w_1}{(w_2 - w_1)b_0} = \frac{w_2(b_1/b_0 - 1) + (b_1/b_0) \left(\frac{w_1^2}{n} - 2w_1\right)}{w_2 - w_1} \\ &= \frac{w_2(K - 1) + K \left(\frac{w_1^2}{n} - 2w_1\right)}{w_2 - w_1}, \\ \mu &= \frac{w_2 b_1 - b_1 w_1 - \left(b_1 - \frac{b_1 w_1}{n}\right) w_2}{(w_2 - w_1)b_0} = \frac{w_2(b_1/b_0) + (b_1/b_0) \left(\frac{w_1 w_2}{n} - w_1 - w_2\right)}{w_2 - w_1} \\ &= \frac{w_2 K + K \left(\frac{w_1 w_2}{n} - w_1 - w_2\right)}{w_2 - w_1}.\end{aligned}$$

Writing μ in the form

$$\mu = \frac{K \left(\frac{w_1 w_2}{n} - w_1\right)}{w_2 - w_1}$$

we see that $\mu = 0$ ($\mu = K$) is equivalent to $w_2 = n$ (resp. $w_1 = n$). But $n|C| = b_1 w_1 + b_2 w_2 < (|C| - |C_0|)w_2$, so $w_2 > \frac{n|C|}{|C| - |C_0|} > n$. Hence $\Gamma(C)$ is trivial iff $\mu = K$ iff $w_1 = n$. \square

REMARK 13. Since $\Gamma(C)$ is a Cayley graph, the preceding argument shows that $\Gamma(C)$ is trivial iff the codewords of weight 0 and w_2 form a linear subcode of C (and the cocliques of $\Gamma(C)$ are the cosets of $(C_0 + C_2)/C_0$ in this case).

4. The Dual of a Modular Two-Weight Code

Suppose $C \leq_R R^n$ is a two-weight code over a finite Frobenius ring with nonzero weights w_1, w_2 and frequencies b_1, b_2 . Let $\mathbf{M}_i \in R^{b_i \times n}$ ($i = 1, 2$) be matrices whose rows are the codewords of C of weight w_i in some order.

DEFINITION 14. The right linear code $C' \leq R_R^{b_1}$ generated by the columns of \mathbf{M}_1 is called the *dual of the two-weight code C* .

The code C' is modular of index 1 (no matter whether C is modular or not).

THEOREM 15. If $C \leq_R R^n$ is a modular two-weight code with $C_0 = \{\mathbf{0}\}$, its dual C' is also a (modular) two-weight code with $C'_0 = \{\mathbf{0}\}$ and nonzero weights

$$w'_1 = \frac{(w_2 - n - r)|C|}{w_2 - w_1} = \frac{b_1 w_1}{n}, \quad w'_2 = \frac{(w_2 - n)|C|}{w_2 - w_1}. \quad (11)$$

PROOF. Suppose C is generated by $\mathbf{G} = (\mathbf{g}_1 | \dots | \mathbf{g}_n) \in R^{k \times n}$. The weight of $\mathbf{d}_i = \mathbf{M}_i \mathbf{y}^T$ ($\mathbf{y} \in R^n$) is $w_{\text{hom}}(\mathbf{d}_i) = \sum_{\mathbf{c} \in C_i} w_{\text{hom}}(\mathbf{c} \cdot \mathbf{y})$. By assumption, $C = C_1 \uplus C_2 \uplus \{\mathbf{0}\}$. Hence we get the following system of equations for $w_{\text{hom}}(\mathbf{d}_1)$ and $w_{\text{hom}}(\mathbf{d}_2)$:

$$\begin{aligned}w_{\text{hom}}(\mathbf{d}_1) + w_{\text{hom}}(\mathbf{d}_2) &= \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c} \cdot \mathbf{y}), \\ w_1 \cdot w_{\text{hom}}(\mathbf{d}_1) + w_2 \cdot w_{\text{hom}}(\mathbf{d}_2) &= \sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(\mathbf{c} \cdot \mathbf{y}).\end{aligned} \quad (12)$$

If $\mathbf{y} \in C^\perp$ then $\mathbf{d}_1 = \mathbf{d}_2 = 0$. Otherwise

$$\begin{aligned}
\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c} \cdot \mathbf{y}) &= |C|, \\
\sum_{\mathbf{c} \in C} w_{\text{hom}}(\mathbf{c}) w_{\text{hom}}(\mathbf{c} \cdot \mathbf{y}) &= \sum_{j=1}^n \sum_{\mathbf{c} \in C} w_{\text{hom}}(c_j) w_{\text{hom}}(\mathbf{c} \cdot \mathbf{y}) \\
&= \frac{|C|}{|R|^k} \sum_{j=1}^n \sum_{\mathbf{x} \in R^k} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}_j) w_{\text{hom}}(\mathbf{x} \mathbf{G} \mathbf{y}^\top) \\
&= |C| \left(n + \frac{\alpha(\mathbf{G} \mathbf{y}^\top R^\times)}{|\mathbf{G} \mathbf{y}^\top R^\times|} \right) \\
&= \begin{cases} (n+r)|C| & \text{if } \mathbf{G} \mathbf{y}^\top \sim \mathbf{g}_j \text{ for some } j, \\ n|C| & \text{otherwise.} \end{cases}
\end{aligned}$$

□

Solving (12) for $w_{\text{hom}}(\mathbf{d}_1)$ in both cases gives (11). As w'_1, w'_2 are positive, we see that $C'_0 = \{\mathbf{0}\}$. Since C is not a one-weight code, there exists $\mathbf{y} \in R^n$ such that $\mathbf{0} \neq \mathbf{G} \mathbf{y}^\top \notin \mathbf{g}_1 R^\times \cup \dots \cup \mathbf{g}_n R^\times$ (cf. Fact 7). Hence both weights w'_1, w'_2 actually occur and the proof of Th. 15 is complete.

THEOREM 16. *Under the assumptions of Th. 15, the graph $\Gamma(C')$ is strongly regular with parameters*

$$N' = |C|, \quad K' = \frac{n}{r}, \quad \lambda' = \frac{2n - w_1 - w_2}{r} + \frac{w_1 w_2}{r^2 |C|}, \quad \mu' = \frac{w_1 w_2}{r^2 |C|}.$$

The graph $\Gamma(C')$ is trivial iff $w_1 = n$ (i. e. iff $\Gamma(C)$ is trivial).

PROOF. Since C' is a modular two-weight code with $C'_0 = \{\mathbf{0}\}$, the graph $\Gamma(C') = \Gamma(C', C'_1)$ is strongly regular. It remains to compute the parameters of $\Gamma(C')$.

The proof of Th. 15 shows that $\mathbf{y} \notin C^\perp$ implies $\mathbf{M}_1 \mathbf{y}^\top \neq \{\mathbf{0}\}$. Hence C is generated by the codewords of weight w_1 , $C^\perp = \{\mathbf{y} \in R^n; \mathbf{M}_1 \mathbf{y}^\top = \mathbf{0}\}$ and $N' = |C'| = |R^n|/|C^\perp| = |C|$. This in turn gives for the frequencies b'_1, b'_2 the system of equations $b'_1 + b'_2 = |C| - 1$, $b'_1 w'_1 + b'_2 w'_2 = b_1 |C|$. Solving for b'_1 we obtain, using $w'_2 - b_1 = \frac{(w_2 - n)|C|}{w_2 - w_1} - \frac{(w_2 - n)|C| - w_2}{w_2 - w_1} = \frac{w_2}{w_2 - w_1}$, $w'_2 - w'_1 = \frac{(w_2 - n)|C|}{w_2 - w_1} - \frac{(w_2 - n - r)|C|}{w_2 - w_1} = \frac{r|C|}{w_2 - w_1}$,

$$K' = b'_1 = \frac{(w'_2 - b_1)|C| - w'_2}{w'_2 - w'_1} = \frac{\frac{w_2}{w_2 - w_1} \cdot |C| - \frac{w_2 - n}{w_2 - w_1} \cdot |C|}{\frac{r|C|}{w_2 - w_1}} = \frac{n}{r}$$

and further

$$\begin{aligned}
\mu' &= \frac{K' \left(\frac{w'_1 w'_2}{n'} - w'_1 \right)}{w'_2 - w'_1} = \frac{\frac{n}{r} \left(\frac{w'_1 w'_2}{b_1} - w'_1 \right)}{w'_2 - w'_1} = \frac{\frac{n w'_1}{r b_1} (w'_2 - b_1)}{w'_2 - w'_1} \\
&= \frac{\frac{w_1}{r} \cdot w_2}{(w'_2 - w'_1)(w_2 - w_1)} = \frac{w_1 w_2}{r^2 |C|}, \\
\lambda' - \mu' &= \frac{K' \left(\frac{w_1'^2}{n'} - 2w'_1 \right) + w'_2 (K' - 1)}{w'_2 - w'_1} - \frac{K' \left(\frac{w'_1 w'_2}{n'} - w'_1 \right)}{w'_2 - w'_1} \\
&= -\frac{K' w'_1}{n'} + K' - \frac{w'_2}{w'_2 - w'_1} = -\frac{\frac{n}{r} \cdot \frac{b_1 w_1}{n}}{b_1} + \frac{n}{r} - \frac{w_2 - n}{r} = \frac{2n - w_1 - w_2}{r}, \\
\lambda' &= (\lambda' - \mu') + \mu' = \frac{2n - w_1 - w_2}{r} + \frac{w_1 w_2}{r^2 |C|}.
\end{aligned}$$

By Th. 12, the graph $\Gamma(C')$ is trivial iff $w'_1 = n'$. But $w'_1 = \frac{b_1 w_1}{n}$ and $n' = b_1$, so $\Gamma(C')$ is trivial iff $w_1 = n$. □

THEOREM 17. Let $C \leq_R R^n$ be a modular linear code over a finite Frobenius ring R generated by $\mathbf{G} = (\mathbf{g}_1 | \dots | \mathbf{g}_n) \in R^{k \times n}$. Let $D \leq R_R^k$ be the right column space of \mathbf{G} . Suppose C has no all-zero coordinate and satisfies $C_0 = \{\mathbf{c} \in C; w_{\text{hom}}(\mathbf{c}) = 0\} = \{\mathbf{0}\}$. Then the following are equivalent:

- (i) C is a homogeneous two-weight code;
- (ii) $\Omega = \mathbf{g}_1 R^\times \cup \dots \cup \mathbf{g}_n R^\times$ is a partial difference set in $(D, +)$ and $\Omega \cup \{\mathbf{0}\}$ is not a submodule of R_R^k .

PROOF. (i) \implies (ii): By Th. 15 the dual C' is a modular two-weight code with $C'_0 = \{\mathbf{0}\}$ and by Th. 16 the graph $\Gamma(C') = \Gamma(C', C'_1)$ is strongly regular, i.e. the set $C'_1 \subset C'$ of codewords of weight w'_1 is a partial difference set in $(C', +)$. Let $\mathbf{M}_1 \in R^{b_1 \times n}$ be the matrix used to define C' ; cf. Def. 14. There exists $\mathbf{X} \in R^{b_1 \times k}$ with $\mathbf{X}\mathbf{G} = \mathbf{M}_1$. The proof of Th. 16 shows that $\mathbf{X}\mathbf{G}\mathbf{y}^\top = \mathbf{M}_1\mathbf{y}^\top = \mathbf{0}$ implies $\mathbf{G}\mathbf{y}^\top = \mathbf{0}$. Hence $f(\mathbf{y}^\top) := \mathbf{X}\mathbf{y}^\top$ defines an right R -module isomorphism f from $D = \{\mathbf{G}\mathbf{y}^\top; \mathbf{y} \in R^n\}$ to $C' = \{\mathbf{M}_1\mathbf{y}^\top; \mathbf{y} \in R^n\}$. Again by the proof of Th. 16, $w_{\text{hom}}(\mathbf{M}_1\mathbf{y}^\top) = w'_1$ iff $\mathbf{G}\mathbf{y}^\top \sim \mathbf{g}_j$ for some j , i.e. iff $\mathbf{G}\mathbf{y}^\top \in \Omega$. In other words, we have $f(\Omega) = C'_1$. Clearly this implies that Ω is a partial difference set in $(D, +)$. The second assertion of (ii) follows from Fact 7.

(ii) \implies (i): Since

$$w_{\text{hom}}(\mathbf{x}\mathbf{G}) = \sum_{\mathbf{g}R \in \mathcal{P}} \alpha(\mathbf{g}R) w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}) = r \sum_{\mathbf{g} \in \Omega} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}),$$

it suffices to show that $\mathbf{x} \rightarrow \sum_{\mathbf{g} \in \Omega} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g})$ takes no more than two nonzero values on R^k .

By [10, Cor. 3.3] there are $v_1, v_2 \in \mathbb{R}$ such that for any nontrivial (complex) character λ of $(D, +)$ we have $\lambda(\Omega) = \sum_{\mathbf{g} \in \Omega} \lambda(\mathbf{g}) \in \{v_1, v_2\}$. If χ is a generating character of R then clearly $D \rightarrow \mathbb{C}^\times$, $\mathbf{g} \mapsto \chi(\mathbf{x} \cdot \mathbf{g})$ is a character of $(D, +)$. Hence

$$\begin{aligned} \sum_{\mathbf{g} \in \Omega} w_{\text{hom}}(\mathbf{x} \cdot \mathbf{g}) &= \sum_{\mathbf{g} \in \Omega} \left(1 - \frac{1}{|R^\times|} \sum_{u \in R^\times} \chi(\mathbf{x} \cdot \mathbf{g}u) \right) \\ &= |\Omega| - \frac{1}{|R^\times|} \sum_{u \in R^\times} \sum_{\mathbf{g} \in \Omega} \chi(\mathbf{x} \cdot \mathbf{g}u) \\ &= |\Omega| - \sum_{\mathbf{g} \in \Omega} \chi(\mathbf{x} \cdot \mathbf{g}) \end{aligned}$$

takes only the values 0 (if $\mathbf{x}\mathbf{G} = \mathbf{0}$), $|\Omega| - v_1$ or $|\Omega| - v_2$. Hence $C = \{\mathbf{x}\mathbf{G}; \mathbf{x} \in R^k\}$ is a two weight code with nonzero weights $w_1 = r(|\Omega| - v_1)$, $w_2 = r(|\Omega| - v_2)$. (By Fact 7 and the assumption that $\Omega \cup \{\mathbf{0}\}$ is not a submodule of R_R^k , it cannot be a one-weight code.) \square

REMARK 18. Under the assumptions of Th. 17 the set $\Omega \cup \{\mathbf{0}\}$ is a submodule of R_R^k iff C is a homogeneous one-weight code, and $D \setminus \Omega$ is a submodule of R_R^k iff C is a homogeneous two-weight code with $w_1 = n$.

References

- [1] E. Byrne, M. Greferath, and T. Honold. Two-weight codes over finite Frobenius rings and strongly regular graphs. In *Optimal Codes and Related Topics*, pages 64–73, Pamporovo, Bulgaria, 2005.
- [2] E. Byrne, M. Greferath, and T. Honold. Ring geometries, two-weight codes, and strongly regular graphs. *Designs, Codes and Cryptography*, 48:1–16, July 2008.
- [3] R. Calderbank and W. M. Kantor. The geometry of two-weight codes. *Bulletin of the London Mathematical Society*, 18:97–122, 1986.
- [4] I. Constantinescu and W. Heise. A metric for codes over residue class rings. *Problems of Information Transmission*, 33(3):208–213, 1997.
- [5] P. Delsarte. Weights of linear codes and strongly regular normed spaces. *Discrete Mathematics*, 3:47–64, 1972.

- [6] M. Greferath and S. E. Schmidt. Finite-ring combinatorics and MacWilliams' equivalence theorem. *Journal of Combinatorial Theory, Series A*, 92:17–28, 2000.
- [7] W. Heise and T. Honold. Homogeneous and egalitarian weights on finite rings. In *Proceedings of the Seventh International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-2000)*, pages 183–188, Bansko, Bulgaria, 2000. Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia.
- [8] T. Honold. Characterization of finite Frobenius rings. *Archiv der Mathematik*, 76(6):406–415, 2001.
- [9] T. Honold and A. A. Nechaev. Weighted modules and representations of codes. *Problems of Information Transmission*, 35(3):205–223, 1999.
- [10] S. L. Ma. A survey of partial difference sets. *Designs, Codes and Cryptography*, 4:221–261, 1994.
- [11] J. A. Wood. Duality for modules over finite rings and applications to coding theory. *American Journal of Mathematics*, 121(3):555–575, 1999.
- [12] J. A. Wood. The structure of linear codes of constant weight. *Transactions of the American Mathematical Society*, 354:1007–1026, 2001.

THOMAS HONOLD, INSTITUTE OF INFORMATION AND COMMUNICATION ENGINEERING, ZHEJIANG UNIVERSITY, ZHEDA ROAD, 310027 HANGZHOU, CHINA

E-mail address: honold@zju.edu.cn